THREATLOCKER®

100 DAYS TO SECURE YOUR ENVIRONMENT

Whether you're starting from zero or organizing an inherited environment, this tactical weekly series will walk you through how to fully secure your environment step by step.

Visit threatlocker.com/100days to view each webinar.

WEEK 1 CHECKLIST:

The first step in protecting your environment is to get visibility over everything—network & file activities, executions, and elevations. Define test groups and deploy your agent of choice.

- □ Deploy test group
  - □ Start monitoring file activity, executions, elevations, and network activity

    If you're not a current ThreatLocker® customer, you can book a 30-minute quick start demo to get access to the ThreatLocker Portal and download the agent. Click here to book a demo with a Solution Engineer. ThreatLocker is not required for this; however, it does make it easier.
  - □ Define test groups to test deployments. This should include a few people from each team department
  - □ Buy them a box of donuts as a thank you
- □ Initial policy adjustments
  - □ Set password protected screen saver
  - □ Turn off Windows keylogger
- □ Identify apps that require local admin access
- □ Document USB drive usage
- □ Document local admin accounts and when these were last logged in

  See week 1 resources for access to PowerShell script
- □ Do a port scan of your network

WEEK 2 CHECKLIST:

Begin auditing critical attack vectors—local admin rights, SMBv1, and USB drive access.

- □ Learn how to search in the Unified Audit
- □ Create USB drive access policies
  - □ Block USB drive access with request to approve
  - □ Consider blocking all non-encrypted USB drives as well as only permitting specific file extensions
  - □ Create an alert and block USB drive access on excessive usage in a short period of time
- □ Briefly review applications in your environment, especially high-risk applications
- □ Remove unused local administrative rights
- □ Implement policies to allow specific programs to run as admin
- □ Disable Office macros
- □ Turn on monitoring for SMBv1
- □ Turn on BitLocker
- □ Purchase domains with similar spelling to your own

WEEK 3 CHECKLIST:

Lock down your internet traffic. That means denying most inbound traffic for workstations and outbound traffic for servers.

- □ Simulate denies for Network Control and Application Control in the Unified Audit
  - □ Start securing machines after simulating denies
- □ Deny inbound traffic on workstations
  - □ Make sure to use dynamic ACLs to automatically allow necessary connections over specific ports
- □ Restrict outbound traffic on servers
  - □ Start with test servers
- □ Block SMBv1
- □ Block SMB ports by default

  If you have ThreatLocker® agent installed and auditing is enabled, refer to the ThreatLocker Community for alerts on SMBv1 usage and guidance on blocking SMB ports by default.

WEEK 4 CHECKLIST:

Protect your cloud. Use MFA where possible, avoiding SMS unless required. Set up and configure Conditional Access to protect your M365 environment.

- □ Turn off your VPN
- □ Use MFA where possible

  Avoid SMS-based MFA unless required
- □ Enable Conditional Access
  - □ Set policies to report-only mode until you're sure

    See the ThreatLocker® webinar on securing your Microsoft 365 environment or read the ebook for a more in-depth analysis
- □ Use your company's branding where possible

WEEK 5 CHECKLIST:

Deploy your agent of choice across the rest of your environment. Begin locking down risky applications—contain risky but necessary applications.

- □ Filter bad web content
- □ Install your agent of choice onto all machines

  Some can be in Learning or Monitor Mode until polices have been tested.
- □ Block risky applications and browser extensions

  Many browser extensions have overly broad permissions.
- □ Contain risky but necessary applications

WEEK 6 CHECKLIST:

Patch everything—your applications, operating systems, and even your router. Backup your data and test them.

- □ Patch your applications & operating system
- □ Patch all other devices—even your router

  For example: In 2018, 70% (1.4 million) of all MikroTik routers were actively hacked. However, a patch had been released months before any were exploited.
- □ Regularly backup your data
  - □ 3 copies of your data in 2 locations, 1 of which is off-site (3-2-1 rule)
  - □ Also verify that they work
- □ Protect your backups

  ThreatLocker Storage Control can restrict file access to only specific software or users.

WEEK 7 CHECKLIST:

Enforce Conditional Access and create dynamic named locations.

- □ Review your report-only policies in M365
  - □ If there have been no false positives, turn them on
  - □ If there have been false positives, try the what-if simulator to adjust the policy

    Be careful with applying policies to your break-glass accounts
- □ Try out ThreatLocker® Cloud Control to dynamically update your named locations to block access to high-value accounts

  The ThreatLocker mobile application enables on-the-go updates when away from your computer

WEEK 8 CHECKLIST:

Protect your macOS computers. While they can use many of the same policies as your Windows workstations, they require specific settings.

- □ Do not disable any of the built-in macOS protections (SIP, Gatekeeper, Firewall, etc.)
- □ Disable AirDrop and only use it when necessary
- □ Enable disk encryption with FileVault
- □ Block all macOS sharing capabilities (Screen, File, Media, etc.) which you don't use or enable them by request only

WEEK 9 CHECKLIST:

Be extra careful approving applications for your servers. Configure additional security checks for your servers.

- □ Be even more restrictive about what applications are allowed compared to workstations
  - □ Set up an alert for when your default-deny policy is triggered
- □ Block most outbound traffic
- □ Allow some inbound traffic

  Dynamic ACLs are a secure way to restrict inbound traffic, especially RDP (port 3389)
- □ Enforce MFA for login
- □ Follow the principle of least privilege where possible

WEEK 10 CHECKLIST:

Your domain controller is important—so protect it. Audit and set policies.

- □ Audit domain accounts
- □ Audit and set fine-grained password policies

  These should be tailored to your organization
- □ Enable Group Policy auditing
- □ Disable mDNS
- □ Enable LDAP signing requirements

  This may break authentication for legacy devices, so test accordingly
- □ Check out Configuration Manager to simplify policy management across domains

WEEK 11 CHECKLIST:

While Zero Trust is the best way to stay secure, it's important to have multiple layers of security. Set up automated responses in your EDR and configure your MDR runbook.

- □ Set up automated responses in your EDR
  - □ Use threat levels to remove access to admin tools and sensitive folders
- □ Create a runbook for MDR
  - □ Endpoint and Cloud
  - □ Be specific on who you want contacted and what to do if no one answers
- □ Check out Cloud Control to stop unauthorized logins to your M365 tenant

  There's also a mobile agent for on-the-go updates

WEEK 12 CHECKLIST:

Review your policies and make sure that only what's needed is allowed.

- □ Review and remove unused policies

  Be careful about applications used in regular intervals
- □ Promote policies to the group or organizational level if used across your environment
- □ Ensure that your USB policies are applied across your organization
- □ Block Telnet
- □ Test your policies to ensure they're setup correctly

WEEK 13 CHECKLIST:

ThreatLocker® released a syslog ingestor to bring SIEM-like capabilities. Disable the new AI-powered feature that will continuously take screenshots of your computer (Windows Recall).

- □ Set up syslog data ingestion
- □ Configure monitored file paths
- □ Restrict access to files upon mass file changes

  This may take some testing to reduce false positives
- □ Disable Windows Recall
- □ Create canary files and alert if they're accessed

WEEK 14 CHECKLIST:

ThreatLocker released Defense Against Configurations (DAC), a free dashboard to detect misconfigurations in your environment.

- □ Enable DAC for your organization (or a test group)

  This can be done by adding "EnableDAC" to your options page
- □ Address any failures according to their criticality
- □ Review related compliance frameworks

About ThreatLocker®

ThreatLocker® is a Zero Trust Endpoint Protection Platform that improves enterprise-level server and endpoint security with Zero Trust controls, including: Allowlisting, Ringfencing™, Storage Control, Network Control, ThreatLocker® Detect, Elevation Control and Configuration Manager.

sales@threatlocker.com

+1-833-292-7732

threatlocker.com